Benefits of Location-Based Access Control: A Literature Study

André van Cleeff, Wolter Pieters, Roel Wieringa
Information Systems
University of Twente
Enschede, The Netherlands
{*a.vancleeff, w.pieters, r.j.wieringa*}*@utwente.nl*

***Abstract*—Location-based access control (LBAC) has been suggested as a means to improve IT security. By 'grounding' users and systems to a particular location, attackers supposedly have more difficulty in compromising a system. However, the motivation behind LBAC and its potential benefits have not been investigated thoroughly. To this end, we perform a structured literature review, and examine the goals that LBAC can potentially fulfill, the specific LBAC systems that realize these goals and the context on which LBAC depends. Our paper has four main contributions: first we propose a theoretical framework for LBAC evaluation, based on goals, systems and context. Second, we formulate and apply criteria for evaluating the usefulness of an LBAC system. Third, we identify four usage scenarios for LBAC: open areas and systems, hospitals, enterprises, and finally data centers and military facilities. Fourth, we propose directions for future research: (i) assessing the tradeoffs between location-based, physical and logical access control, (ii) improving the transparency of LBAC decision making, and (iii) formulating design criteria for facilities and working environments for optimal LBAC usage.**

***Keywords*-location-based access control; LBAC; context-sensitive access control**

I. Introduction

The automation of business processes moves events from the physical to the digital domain. We automate because IT embodies desirable characteristics that are not present in the physical domain, or because it lacks undesirable characteristics present in the physical domain. Unfortunately, IT not only takes away undesirable physical characteristics, it also takes away desirable properties, thereby causing security problems. These problems are normally dealt with in the same digital domain, where logical access control prevents unauthorized access by users.

To mitigate the deficiencies of logical security mechanisms, and coinciding with the trend of cyber-physical systems, security mechanisms have been proposed that integrate with the physical environment. In so-called location-based access control (LBAC), a system infers the location of a principal through sensors and takes it as input for access control decisions [1]. This allows for the specification and enforcement of location-specific security policies, for example restricting access of sensitive data to a specific room. LBAC is part of the family of context-sensitive access control systems [2], which take all sorts of contextual information as input.[1]

Intuitively, LBAC can improve security, because a user's location is correlated to the access rights she is entitled to. A manager in an enterprise has no need for confidential customer data outside of her office, and access to this data from outside is thus likely malicious.

However, although the benefits of LBAC are intuitively easily understood, its research and application are hindered by the fact that there is no clear theory that explains how precisely LBAC integrates with and depends on the environment [3]. Hulsebosch et al. [2] argued that benefits mainly depend on the value of the resources that LBAC protects, but no general framework exists for deciding which LBAC model is more suitable in which context or for which resource, or in fact, explaining why LBAC actually improves access control at all.

In this paper, we take on this challenge of uncovering the actual benefits of LBAC, and present the results of a structured literature review on LBAC. We try to answer two questions:

1) To what extent can LBAC achieve access control goals?
2) In what context is LBAC useful?

Section II explains our research approach. Access control goals are discussed in Section III, LBAC systems in Section IV and the context in which LBAC operates in Section V. Finally conclusions about the usefulness of LBAC are drawn in Sections VI and VII.

Our paper has four contributions: first, we develop a theoretical framework for its evaluation, based on goals, systems and context. Second, we evaluate the usefulness of LBAC based on five criteria: least privilege, separation of duty, accountability, usability and maintainability. Third, we identify usage scenarios for practitioners. As a fourth contribution, we propose directions for further research.

II. Research methodology

In evaluating LBAC, we faced two methodological challenges: (i) setting up the literature study, and (ii) developing a theoretical framework for understanding the benefits of LBAC. We will discuss each of these in detail.

[1]There are many terms for these types of systems, which are all put under the 'flag' of LBAC, because this term is most widely used and covers our research best.

A. Literature study

The study's scope was limited to scientific literature found on Scopus[2], including the majority of IEEE, ACM, Springer and Elsevier publications in conferences and journals. We followed the structured literature review method of Webster and Watson [4], except for the literature search itself. Rather than examining journal papers and moving backwards to the references, and forward to citations in conferences and workshops, we applied straightforward keyword search criteria. Concerning the presentation of results, we did follow the approach from Webster and Watson to categorize the results by concept rather than by author, to identify strengths and weaknesses (for example research gaps) in the existing research.

Literature selection was done in three steps. First, we identified relevant keywords to search for, starting with an initial search for "Location-Based Access Control" in titles, abstracts and keywords of papers. Generally, similar terms can be split in two parts: a part on context (such as spatio-temporal), and one part on identity and access control (such as role-based access control). This is shown in Figure 1. In total we created $7 \times 5 = 35$ keyword combinations.

Context term	Access control term
Context-sensitive	Authentication
Context-aware	Authori(s/z)ation
Context-dependent	Access control
Location-based	Role-based access control
Location-aware	RBAC
Spatio(-)temporal	
Proximity-based	

Figure 1. Search terms

In the second step, we found 159 papers with these keywords, which were retrieved in the third step using Google Scholar[3]. We excluded non-retrievable or irrelevant papers, resulting in 99 full papers.

In our initial investigation of LBAC, we noticed that most papers did not present any clear motivation for LBAC usage. Instead they presented LBAC models and examples of their usage. To include literature lacking explicit motivations, we attempted to derive these by following the grounded theory method [5], which allows the development of a theory based on collected data in a structured manner. We collected two types of information:

1) Models of LBAC, how the authors conceptualized relevant events and properties of space-time.
2) Motivating examples on LBAC usage. In total 91 motivational examples were found.[4]

[2]www.scopus.com

[3]scholar.google.com

[4]These examples will be made available in our technical report from eprints.eemcs.utwente.nl/.

B. Theoretical framework

We use the system engineering argument to create a theory on the benefits of security mechanisms: S and A entail E, where S is the system, A are the assumptions and E the emergent properties of the system [6]. In line with common LBAC terms, we will here use the terms (LBAC) system, context and goal. Figure 2 shows the relation between these three terms and we explain them in more detail.

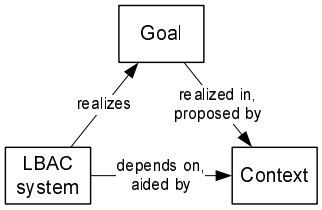

Figure 2. The relation between goals, system and context.

1) Goals: Our objective is first to learn what types of goals LBAC can contribute to, including adherence to certain security principles such as that of least privilege. Goals are discussed in Section III.

2) Systems: Concerning the LBAC system, we investigate what models (conceptual representation of locations) exist, and how they represent context. We view LBAC systems simply as functions with an input consisting of time, subjects, objects and their locations, and have as output an access control decision, focusing on how LBAC systems use contextual information about these inputs in decision making. As such, we exclude implementations details of LBAC from our research. Systems are discussed in Section IV.

3) Context: Concerning the context, we are interested in how LBAC interacts with its environment. Interaction consists of three types:

- context as a source of *requirements* for LBAC
- *dependencies* of the LBAC system on the context
- *contributions* of the context on realizing the goals

To evaluate the dependencies on the physical environment we will use the concepts of *imposed* versus *inherent* properties [7]: logical access control restrictions are logically *imposed* on systems, whereas physical access control systems (such as fences and walls) are subjected to *inherent* physical laws, making them resilient to attacks in a different way. Dependencies on these properties will be discussed in Section V.

In the next sections we will discuss goals, systems and context in the classic top-down requirements engineering approach: first we list the goals, then the systems that realize those goals and finally the context in which the system is placed, and how it interacts with it.

III. Goals

In information security, goals relate to confidentiality, integrity and availability of data. These are in turn realized by security services, such as access control. Access control protects resources against inappropriate or undesired user

access. This requires selective sharing of information [8]: neither granting nor denying access to everyone leads to a useful access control system. Access control is comprised of three services:

- identification: uniquely identifying principals
- authentication: verifying the identity of a principal[5]
- authorization: determining if a principal has access rights

These services depend on each other: without managing identities, one cannot authenticate a principal, and checking authorizations requires knowledge and proof of her identity. In this paper, we focus on authorizations, but because of the aforementioned dependencies, we also pay attention to some issues concerning identification and authentication.

Most access control types in IT systems are logical, and typically have an authorization function $f : Subject \times Object \times Action \rightarrow \{yes, no\}$ where a subject requests permission to perform an action[6] on an object. Inside the function f the decision making takes place. A widely used logical access control model is role-based access control (RBAC) [10].

Decker gives specific LBAC requirements [11], including the ability to specify

- 'abstract' locations: such as an 'office room' rather than plain geometric structures
- 'dynamic location restrictions': for example, limit access to a document to the room where the user created it
- how to deal with imperfect measurements of a user's location

Sandhu et al. specifically mention the principles of least privilege and separation of duty [10], whereas Hu et al. state that there are no well-accepted metrics [8]. Instead usefulness depends on the context and the needs of the organization using it. In total, Hu et al. list 14 specific criteria, including the aforementioned two principles.

As LBAC goals, we use adherence to the principles of least privilege and separation of duty, as these are widely accepted access control goals, and also include one quality criterion from Hu et al., namely maintainability. As a fourth and fifth criteria, we include accountability and usability, as these are important for pervasive systems. These five goals are next discussed in more detail.

A. Principle of separation of duty

Because principals are not always trustworthy, actions must be split between principals, allowing each one to verify the other, or depend on the other for execution. Separation of duty (SoD) is possible in time (workflow), or using a two-man or dual control policy, which requires multiple persons to approve an action. Toahchoodee and Ray [12] list two types of SoD: static SoD means that users do not have conflicting roles or permissions, dynamic SoD means that users cannot activate conflicting roles during the same session.

[5]Cf. Denning and MacDoran for an early proposal for location-based authentication [9].

[6]The term operation instead of action is also used.

B. Principle of least privilege

In theory, access control allows the implementation of the principle of least privilege [13]: access to resources should only be granted when necessary for legitimate purposes. Implementation of this principle limits the risks: First, it prevents actors from making mistakes when they have too many authorizations. Secondly, it prevents malicious actors from abuse, as they cannot access everything. Third, it prevents anyone impersonating the actor (for example because of password theft) from accessing more data than the actor was entitled to see.

C. Accountability

In practice, the principle of least privilege is hard to implement, because no one knows precisely what access rights are necessary for legitimate purposes. Instead, users should be held accountable for their actions [14]. This is done by logging and monitoring these actions. It can also act as a deterrence, and in some case even allow recovery from illegal actions.

D. Maintainability

The problem of adherence to the principle of least privilege leads to a fourth goal, namely maintainability. Administrators must keep track of what users are authorized to do, and keep authorizations synchronized to their job descriptions.

E. Usability

Finally, an access control system that puts a heavy burden on its users will likely be circumvented. For example a system that requires many role switches and passwords will likely be circumvented by users and defeat its purpose.

IV. Systems

After discussing the goals for LBAC, we now examine the LBAC systems themselves. More precise, we investigate the types of conceptual LBAC models that exist, and how they take location into account for their access control decisions. As mentioned in Section II, we exclude implementations and their vulnerabilities from our research. This is not to say that these are trivial. For example when a PDA serves as a proxy for a person, and is granted permissions, it can still be stolen, no longer signaling the location of the owner. One specific implementation problem for LBAC systems is preserving the privacy of users: determining who has access to the context of the user [2]. Without denying the complexity of this problem, we assume that this problem can be solved.

To examine the LBAC systems, we first consider how to represent 'context' and how it can be split in low-level and high-level concepts. Next, we look at LBAC as a simple access control function, and examine what inputs it potentially can have. Finally we examine how different LBAC models make decisions.

A. Representing the context

1) Defining the context: LBAC systems are a form of context-sensitive access control. Context is defined as "any information that is useful for characterizing the state or the activity of an entity or the world in which this entity operates" [15]. Context is first read from sensors and these inputs can be used to infer high-level context [16]. For example, social behavior of subjects (such as a doctor accompanying a patient), can be inferred from observing the locations of individuals [17]. Context can be split in low-level and high-level context.

2) Low-level context: Low-level context consists of Cartesian (x,y), (x,y,z) or GPS coordinates. These coordinates are then translated to logical positions (addresses and facilities) by LBAC systems such as GEO-RBAC [18] or STRBAC [19]. A specific logical location type is a country, which has specific legislation [20]. Next to locations, objects are also defined, either physical or logical [21]. As entities move, access decisions also depend on time, it does not only matter *where* an entity is but also *when*, for example restricting employees to access data only on the premises of a facility and during working hours. Generalized Temporal Role Based Access Control (X-GTRBAC) [22] is an example of an LBAC system that considers time intervals, and limited duration of access.

3) Higher-order context: On top of logical locations, Zhang et al. [23] also model the hierarchical containment relations between locations, as well as their proximity. GEO-RBACC is an extension of GEO-RBAC, supporting continuous monitoring of users to infer trajectories. Authorizations can be revoked if users leave a location [18]. Several authors consider position, movement and/or interaction between entities [1], [18], [24]. Ardagna et al. use five predicates to define the context status: *disjoint, distance, velocity, density, location density* [1].

B. Access control model

Generally, LBAC models determine access of a subject to an object, considering only the location of the subject. In many cases, the object location is static [20], but for example in case of providing passengers in a moving train with Internet access, the object accessed is also moving [2]. Another exception are Park et al., who motivate the inclusion of object location in LBAC for safety reasons [25]. LBAC models can thus use different types of locations [26]: In most cases, the subjects are persons and the objects consist of data or systems at a remote location. An example of an LBAC system that directly impacts the user's device is given by Schmidt et al. [27], who propose to disable a camera in a sensitive location. Obviously, access control rules based on subjects and objects can be generalized, for example only allowing access to a medical file when a doctor and a patient are in the same consulting room [17].

C. Decision making model

Most LBAC security models apply a form of RBAC [21], [26], [28]–[30]. Apart from having a certain role, a user then also needs to be in a certain location to perform an action, or activating roles is only possible in a certain location. These models can also be extended with specific time restrictions, leading to spatial and temporal access control [19], [31], [32]. Such models optionally take the movement of persons into account (movement-aware access control). Spatio-Temporal RBAC is formalized by Toahchoodee and Ray [12].

An alternative for RBAC schemes is to use mandatory access control (MAC) [33]: objects and locations have certain security levels. Here, moving a highly sensitive device into a low level security zone will disable its features. For example, a computer with top secret information will not work in a public place. Ray and Yu [21] restrict access to location information using a MAC model. Objects must be contained by locations with higher clearance levels.

Apart from role-based and mandatory access control decision models, state checking matrices (SCM) [34], predicates [35], and automata [36] are also proposed.

D. General LBAC model

Figure 3 illustrates how LBAC systems represent and reason with context.

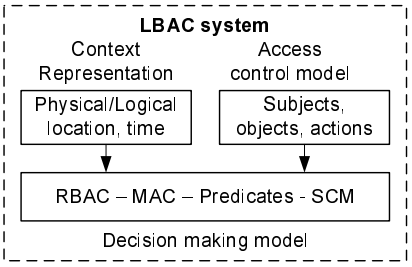

Figure 3. Internal model of an LBAC system

Basic contextual elements of LBAC systems include physical and logical locations. In logical access control, subjects wish to perform operations on an object. In the case of LBAC, there are reasons to generalize such access control decisions, and take the location of multiple subjects and objects into account. Higher-level context includes history, trajectory of entities, and their closeness, legal status and social behavior.

V. Context

Contrary to the previous section, in which we investigated how LBAC models can *represent* the context, we will now investigate the context *surrounding* LBAC, to assess for which situations LBAC is suitable and why. The context provides three types of motivations for using LBAC:

1) as a source of *requirements*
2) as a *dependency* of LBAC
3) as a *contribution* to realizing security goals

First, a context (such as the usage of pervasive systems) places specific demands on an access control system. Second, a system can depend on specific properties of the context, such as that users move through buildings no faster than walking speed. Third, contextual factors can improve the workings of LBAC, such persons working in different locations. Figure 4

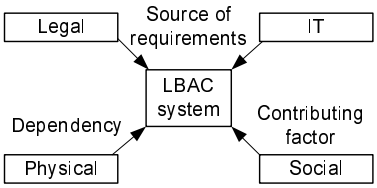

Figure 4. The context of an LBAC system

shows that the LBAC system context can be split into four parts:

- IT context: systems that require access control
- physical context: buildings, rooms and other physical security mechanisms
- social context: behavior of people working and living in physical structures
- legal context: the juridical framework overlying the other contexts

These parts have some overlap, but are to a large extent independent. For each of these, we explain in more detail how this context relates to the goals and systems.

A. IT context

Pervasive or ubiquitous systems, that use sensors, wireless transmissions and/or movable devices, differ from normal systems in their access control requirements. User actions should affect access control on objects [37] and because the actions are determined by specific locations, this provides a motivation for LBAC.

Hulsebosch et al. argue that in ad-hoc collaborations between users and devices, access control depends more on the context (such as location), and less on identity [2]. Here LBAC can reduce for example the dependency on long passwords. In pervasive systems, identities are either unknown a priori or untrustworthy and cannot be used for standard RBAC [15]: access control should adapt itself to the context.

B. Physical context

The resistance of security functions against attacks commonly rests on problems that are either hard or impossible to solve. For example, in CP-ABE access control, which uses cryptographic functions to enforce access control [38], an assumption is that finding the 'discrete logarithm' is a hard problem. Likewise, a logical access control system, using roles can be formally proven to be correct. Logical access control depends on *imposed* properties, because the hardware on which it executes can potentially do much more. However, LBAC depends on the *inherent* hard problem of achieving certain physical states [39]. For example, persons cannot make themselves invisible or walk through walls. Because of this, employees can keep an eye on each other to prevent unauthorized access, and easily detect outsiders in the office. Properties and states are now discussed in more detail.

1) Physical properties: Physical structures such as buildings are hard to change, even with demolition equipment. This concerns the inertness, containment and reachability properties.[7] First, physical objects do not move by themselves, they are *inert*: In many motivating examples for LBAC the underlying assumption is that devices cannot move by themselves, and require manual intervention, which makes access a 'physical captcha' [41]. Second, the *containment* and *reachability* relation are hard to chance: we cannot suddenly move a room from one building to another or tear down a wall. Physical access control (PAC) can also be a dependency for implementing LBAC.

2) Person properties: Persons are *visible* by others. Because a person's location is relevant for access control decisions, the observation of a person also conveys security-relevant information. If proximity-based access control is used, persons can observe others standing close by, inferring who is accessing their data. Unlike computer viruses or bots, persons have *travel limitations*, and this limits hackers from remote locations in their possibilities. We can also detect malicious access, as a person cannot be in China and Europe at the same time.

3) Combined physical and person properties: LBAC can be used to reduce the chance of a denial-of-service attack, because an authorized location has a *limited capacity* for seating persons. Even when an attack takes place, the attacker can be found in that location.

C. Social context

LBAC is aided by the organization of work, especially the specialization of labor: working activities repeatedly take place in the same locations and time periods. Jobs can be limited to specific hours [42] and such facts can be used by LBAC mechanisms to implement space and time constraints. The proximity of persons to each other also impacts the need-to-know and need-to-do:

- Being alone can improve confidentiality of data, such as in a voting process, where a voter has to fill in a ballot herself, without anyone else being present.
- Being together can make actions more secure because there is more oversight, such as in a 'no-lone zone'. For example, in an election, the voter must cast the ballot in presence of observers, to make sure that she puts only one ballot in the ballot box.[8]

In other situations, social collaborations are ad hoc, and users do not have a specific identity known to the system or each other, or are unauthorized for a specific task. For example in a conference room, participants can send questions to a panel, which has not authorized the participants individually. In such cases, LBAC is still useful because it improves the accountability of persons, limits the chance of denial-of-service attacks and is easy to maintain and use.

[7] Cf. physical modeling [40]

[8] Cf. the concept of natural surveillance [43]

D. Legal context

Although not widely discussed in the literature, the legal context provides an important motivation for LBAC [20]. Different countries have different regulations in place, and LBAC can help to enforce these.

E. Summary of LBAC context

The context of LBAC systems can be split into an IT, physical, social and legal context. The IT and the legal context mainly act as a source of requirements: pervasive systems and laws and regulations require a form of LBAC system. In turn, LBAC depends on physical properties including visibility and inertness. The social context can also contribute to how LBAC functions effectively: if persons move frequently between locations, and interact with each other, LBAC works better. Figure 5 summarizes the relation of LBAC with its context.

Context	Motivation	Key indicators
IT	requirement	pervasive systems
Physical	dependency	inertness, containment, reachability, visibility, travel and speed limits, capacity, PAC
Social	contribution	work environment, collaborations, privacy
Legal	requirement	data protection and business regulations

Figure 5. Context types, motivations and key indicators.

VI. Evaluation

After discussing LBAC goals, systems and the context in which it functions, we will now evaluate LBAC based on two criteria:

1) its achievement of general access control goals
2) its main use cases, in which context it is useful

A. Achievement of goals

1) Least privilege: If well configured, LBAC can increase adherence to the principle of least privilege, as several LBAC models are very fine-grained, allowing a user access only in a specific room or while being in proximity of specific people. One particular problem is automatically granting access to resources: Gupta et al. mention proximity-based access control, and the problem of accidentally granted access [44]: as a user passes by a resource, and is automatically granted access, this violates the principle of least privilege.

2) Separation of duty: LBAC helps to achieve the principle of separation of duty. First, it can require physical separation between users, so that they cannot collude directly. Secondly, LBAC can also require the opposite: two users need to be in the same room to supervise each other.

3) Accountability: LBAC improves accountability, by requiring a user to be in a certain location to use her authorizations. Malicious usage is detectable when someone visits a location she normally does not, and identity theft is deterred because access requires an attacker to visit a location herself, risking detection.

4) Maintainability: LBAC maintainability is mostly ignored in the literature [45]. An exception is GEO-RBAC where maintenance is split between specific spatial domains and subdomains. The resulting problems are similar to those in inter-organizational context, where organizations use federated identity and access control systems. LBAC does not solve these problems, but adds a layer of complexity, namely managing physical spaces. Hulsebosch et al. [2] state that in any context-sensitive access control system, many different parties will control a part of the context. Thus, a-priori, there is little reason to believe that LBAC systems are easier to maintain than their logical counterparts. However, similar to RBAC where roles are given permissions rather than to individual users, LBAC can improve maintainability by granting permissions to locations rather than to individual users. It can also save administrators time when users and devices in dynamic environments can automatically determine authorizations based on their location.

5) Usability: Sastry et al. [46] argue that LBAC is easy, natural, and familiar in the physical world. They give the example of turning on or off lights in a room: this requires being physically present in the room. As such, LBAC can make access control easier and more natural.

Because the location is correlated with a user's identity, LBAC can lower the requirements for authentication. This makes LBAC systems easier to use, especially for always-on systems, such as in hospitals: simply by being close to the system, a doctor can authenticate herself without having to type a long password.[9]

A drawback of LBAC can be that it forces persons to move from one location to the other. During course of the normal activities (such as meeting a patient) this is acceptable, but otherwise hinders usability.

Damiani et al. [45] discuss the problem of 'domain awareness', similar to the problem of accidental access mentioned earlier by Gupta et al.: a traveler might connect to many different systems and must be made aware of this, without being bothered too much.[10] To solve this, Kirkpatrick and Bertino [48] propose to use *enabled* and *activated* roles: the first are possible, and the latter require a specific location or a user action. Furthermore, we consider the problem of transparency: Kirkpatrick and Bertino state that contextual factors include facts that the user cannot know. If that is the case, this certainly reduces usability.

B. Contextual motivating factors

Finally, we evaluate how LBAC benefits from context. First, concerning IT, LBAC is often motivated because logical access control does not work well in an ubiquitous computing context; As the principals are initially unknown, they should be granted access dynamically, based on their location. Second, LBAC depends on the physical environment and physical properties, such as that persons cannot walk through walls.

[9] Cf. continuous authentication systems [47]

[10] Cf. the problems of notifying travelers of changes in roaming fees of mobile phone networks.

Use case	1: Open areas and systems	2: Hospitals	3: Enterprises	4: Data centers and military facilities
Typical application	conference, museum	electronic medical files	enterprise systems	physical maintenance
Main goals	usability	least privilege	accountability, maintainability, usability	separation of duty
main LBAC variant	proximity	RBAC	safety net	MAC
context representation	distance, proximity	rooms, collaboration	buildings, countries	facilities, rooms
IT context	pervasive systems	-	-	-
Physical context	visibility, capacity, reachability	containment, visibility, reachability	containment, PAC, reachability	containment, travel and speed limits, PAC, inertness
Social context	ad hoc	known workforce, close collaboration	known workforce	known workforce, close collaboration
Legal context	-	compliance with privacy regulations	compliance with business rules and data protection	-

Figure 6. Main use cases for LBAC

Third, the social situation contributes to LBAC, for example when there are many persons working in a particular location who can monitor each other's access. Fourth, the legal context can also motivate LBAC usage, to prevent access from specific countries.

Combined, we see four main use cases of LBAC:

1) dynamic or pervasive systems with few security requirements, such as used in conferences or public places
2) static high-security environments with high privacy requirements such as hospitals
3) normal business environments that require a safety net for compliance purposes
4) static high-security environments with physical access control (PAC) such as military facilities

For each of these scenarios, Figure 6 shows the typical IT applications, the main goals that can be achieved, the specific LBAC variant that is most applicable and finally the relation to the context.

VII. Conclusions

In this paper we have examined the benefits of LBAC, by examining the goals it can achieve, the particular models that implement it, and the context on which it depends or which motivates its usage. Our paper has four main contributions:

First, to the best of our knowledge, we have performed the first literature review on LBAC systems, which we based on a theoretical framework using goals, systems and context. We identified four relations between LBAC and its context:

1) context as represented inside LBAC
2) IT and legal context as a source of requirements for LBAC
3) physical context as a source of dependencies for LBAC
4) social context as a contributing factor to achieving goals of LBAC

Second, we formulated and applied two criteria for evaluating the usefulness of LBAC:

1) the extent to which LBAC can achieve general access control goals
2) the context in which LBAC is most useful

Third, we list four usage scenarios for LBAC: open areas and systems, hospitals, enterprises, and finally data centers and military facilities.

As a final fourth contribution, we propose three directions for further research: first, examine the tradeoffs between location-based, physical and logical access control. Especially maintainability of these systems has not been researched extensively. A second unsolved problem is transparency: how to inform users of applicable policies, and how to do the tradeoff analysis between usability and security with respect to automatic activation of authorizations. Third, the existing literature assumes that LBAC is applied in an existing site, but it is not clear how a physical and social structure of a facility should be designed with LBAC in mind.

Acknowledgment

This research is supported by the research program Sentinels (www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs under project number TIT.7628.

References

[1] C. Ardagna, M. Cremonini, E. Damiani, S. di Vimercati, and P. Samarati, "Supporting location-based conditions in access control policies," in *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*. ACM, 2006, p. 222.

[2] R. Hulsebosch, A. Salden, M. Bargh, P. Ebben, and J. Reitsma, "Context sensitive access control," in *Proceedings of the tenth ACM symposium on Access control models and technologies*. ACM New York, NY, USA, 2005, pp. 111–119.

[3] M. Damiani, H. Martin, Y. Saygin, M. Spada, and C. Ulmer, "Spatio-temporal access control: challenges and applications," in *Proceedings of the 14th ACM symposium on Access control models and technologies*. ACM, 2009, pp. 175–176.

[4] J. Webster and R. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly*, vol. 26, no. 2, pp. 13–23, 2002.

[5] J. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative sociology*, vol. 13, no. 1, pp. 3–21, 1990.

[6] R. Wieringa, *Design Methods for Reactive Systems: Yourdon, Statemate, and the UML*. Morgan Kaufmann, 2003.

[7] B. Blakley, "The Emperor's old armor," in *Proceedings of the 1996 workshop on New Security Paradigms*. ACM, 1996, p. 16.

[8] V. Hu, D. Ferraiolo, and D. Kuhn, "Assessment of access control systems," *Interagency Report*, vol. 7316, pp. 20 899–8930, 2006.

[9] D. Denning and P. MacDoran, "Location-based authentication: Grounding cyberspace for better security," *Computer Fraud & Security*, vol. 1996, no. 2, pp. 12–16, 1996.

[10] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[11] M. Decker, "Requirements for a location-based access control model," in *Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia*. ACM, 2008, pp. 346–349.

[12] M. Toahchoodee and I. Ray, "On the formal analysis of a spatio-temporal role-based access control model," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5094 LNCS, pp. 17–32, 2008.

[13] J. Saltzer and M. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975.

[14] J. Cederquist, R. Corin, M. Dekker, S. Etalle, J. den Hartog, and G. Lenzini, "Audit-based compliance control," *International Journal of Information Security*, vol. 6, no. 2, pp. 133–151, 2007.

[15] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila, "A semantic context-aware access control framework for secure collaborations in pervasive computing environments," *The Semantic Web-ISWC 2006*, pp. 473–486, 2006.

[16] R. Bhatti, B. Shafiq, M. Shehab, and A. Ghafoor, "Distributed access management in multimedia IDCs," *Computer*, vol. 38, no. 9, pp. 60–69, 2005.

[17] M. Oh, J. Lee, B. Chang, J. Ahn, and K. Doh, "A programming environment for ubiquitous computing environment," *ACM SIGPLAN Notices*, vol. 42, no. 4, pp. 14–22, 2007.

[18] M. Damiani, E. Bertino, and C. Silvestri, "Approach to Supporting Continuity of Usage in Location-Based Access Control," in *12th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2008. FTDCS'08*, 2008, pp. 199–205.

[19] M. Kumar and R. Newman, "Strbac - an approach towards spatio-temporal role-based access control," in *Proceedings of the Third IASTED International Conference on Communication, Network, and Information Security, CNIS 2006*, 2006, pp. 150–155.

[20] M. Stieghahn and T. Engel, "Law-aware access control for international financial environments," in *Proceedings of the Eighth ACM International Workshop on Data Engineering for Wireless and Mobile Access*. ACM, 2009, pp. 33–40.

[21] I. Ray and L. Yu, "Short paper: Towards a location-aware role-based access control model," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. IEEE Computer Society, 2005, pp. 234–236.

[22] R. Bhatti, E. Bertino, and A. Ghafoor, "A trust-based context-aware access control model for web-services," *Distributed and Parallel Databases*, vol. 18, no. 1, pp. 83–105, 2005.

[23] H. Zhang, Y. He, and Z. Shi, "A formal model for access control with supporting spatial context," *Science in China Series F: Information Sciences*, vol. 50, no. 3, pp. 419–439, 2007.

[24] W. Jansen, S. Gavrila, and V. Korolev, "Proximity-based authentication for mobile devices," in *Proceedings of The 2005 International Conference on Security and Management, SAM'05*, 2005, pp. 398–404.

[25] S. Park, J. Cho, Y. Han, and T. Chung, "Design and Implementation of Context-Aware Security Management System for Ubiquitous Computing Environment," in *Frontiers of High Performance Computing and Networking ISPA 2007 Workshops*. Springer, 2007, pp. 235–244.

[26] M. Damiani and C. Silvestri, "Towards movement-aware access control," in *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*. ACM, 2008, pp. 39–45.

[27] A. Schmidt, N. Kuntze, and J. Abendroth, "Trust for location-based authorisation," in *IEEE Wireless Communications and Networking Conference, WCNC*, 2008, pp. 3163–3168.

[28] J. Joshi, R. Bhatti, E. Bertino, and A. Ghafoor, "Access-control language for multidomain environments," *IEEE Internet Computing*, pp. 40–50, 2004.

[29] A. Muhlbauer, R. Safavi-Naini, F. Salim, N. Sheppard, and M. Surminen, "Location constraints in digital rights management," *Computer Communications*, vol. 31, no. 6, pp. 1173–1180, 2008.

[30] I. Ray, M. Kumar, and L. Yu, "LRBAC: A Location-Aware Role-Based Access Control Model," *Lecture Notes in Computer Science*, vol. 4332, p. 147, 2006.

[31] S. Chandran and J. Joshi, "LoT-RBAC: A location and time-based RBAC model," *Web Information Systems Engineering–WISE 2005*, pp. 361–375, 2005.

[32] I. Ray and M. Toahchoodee, "A spatio-temporal role-based access control model," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4602 LNCS, pp. 211–226, 2007.

[33] I. Ray and M. Kumar, "Towards a location-based mandatory access control model," *Computers & Security*, vol. 25, no. 1, pp. 36–44, 2006.

[34] Y. Kim, C. Mon, D. Jeong, J. Lee, C. Song, and D. Baik, "Context-aware access control mechanism for ubiquitous applications," *Advances in Web Intelligence*, pp. 236–242, 2005.

[35] Y. Shim, "Distributed Processing of Context-Aware Authorization in Ubiquitous Computing Environments," *Computational Science and Its Applications-ICCSA 2006*, pp. 125–134, 2006.

[36] S. Chen, Y. Zhang, and W. Trappe, "Inverting sensor networks and actuating the environment for spatio-temporal access control," in *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*. ACM, 2006, p. 12.

[37] V. Hourdin, J. Tigli, S. Lavirotte, G. Rey, and M. Riveill, "Context-sensitive authorization in interaction patterns," in *Proceedings of the 6th International Conference on Mobile Technology, Application & Systems*. ACM, 2009, pp. 1–8.

[38] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy, 2007. SP'07*, 2007, pp. 321–334.

[39] P. van Oorschot and S. Stubblebine, "Countering identity theft through digital uniqueness, location cross-checking, and funneling," *Financial Cryptography and Data Security*, pp. 31–43, 2005.

[40] T. Dimkov, W. Pieters, and P. Hartel, "Portunes: representing attack scenarios spanning through the physical, digital and social domain," *ARSPA-WITS, Springer*, pp. 112–129, 2010.

[41] P. Golle and N. Ducheneaut, "Preventing bots from playing online games," *Computers in Entertainment (CIE)*, vol. 3, no. 3, p. 3, 2005.

[42] E. Bertino, P. Bonatti, and E. Ferrari, "TRBAC: a temporal role-based access control model," in *Proceedings of the fifth ACM workshop on Role-based access control*. ACM, 2000, pp. 21–30.

[43] T. Crowe and D. Zahm, *Crime prevention through environmental design*. Butterworth-Heinemann Boston, 2000.

[44] S. Gupta, T. Mukherjee, K. Venkatasubramanian, and T. Taylor, "Proximity based access control in smart-emergency departments," in *Proceedings - Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2006*, vol. 2006, 2006, pp. 512–516.

[45] M. Damiani, E. Bertino, and C. Silvestri, "Spatial Domains for the Administration of Location-based Access Control Policies," *Journal of Network and Systems Management*, vol. 16, no. 3, pp. 277–302, 2008.

[46] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM workshop on Wireless security*. ACM, 2003, p. 10.

[47] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE transactions on pattern analysis and machine intelligence*, pp. 687–700, 2007.

[48] M. Kirkpatrick and E. Bertino, "Context-Dependent Authentication and Access Control," *iNetSec 2009–Open Research Problems in Network Security*, pp. 63–75, 2009.